SPECTRUM®

ESX Devices
Management Module Guide

CABLETRON SYSTEMS
SYSTEMS
The Complete Networking Solution™

Summary of Changes

Version	Date	Reason/Rational	Nature of Changes

Notice

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

Printed in the United States of America.

Order Number: 9031586 E3

Cabletron Systems, Inc.
P.O. Box 5005
Rochester, NH 03866-5005

Virus Disclaimer

Cabletron has tested its software with current virus checking technologies. However, because no anti-virus system is 100% reliable, we strongly caution you to write protect and then verify that the Licensed Software, prior to installing it, is virus-free with an anti-virus system in which you have confidence.

Restricted Rights Notice

(Applicable to licenses to the United States Government only.)

1. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

   Cabletron Systems, Inc., 35 Industrial Way, Rochester, New Hampshire 03866-5005.

2. (a) This computer software is submitted with restricted rights. It may not be used, reproduced, or disclosed by the Government except as provided in paragraph (b) of this Notice or as otherwise expressly stated in the contract.

   (b) This computer software may be:

   (1) Used or copied for use in or with the computer or computers for which it was acquired, including use at any Government installation to which such computer or computers may be transferred;

   (2) Used or copied for use in a backup computer if any computer for which it was acquired is inoperative;

   (3) Reproduced for safekeeping (archives) or backup purposes;

   (4) Modified, adapted, or combined with other computer software, provided that the modified, combined, or adapted portions of the derivative software incorporating restricted computer software are made subject to the same restricted rights;

   (5) Disclosed to and reproduced for use by support service contractors in accordance with subparagraphs (b) (1) through (4) of this clause, provided the Government makes such disclosure or reproduction subject to these restricted rights; and

   (6) Used or copied for use in or transferred to a replacement computer.

   (c) Notwithstanding the foregoing, if this computer software is published copyrighted computer software, it is licensed to the Government, without disclosure prohibitions, with the minimum rights set forth in paragraph (b) of this clause.

   (d) Any other rights or limitations regarding the use, duplication, or disclosure of this computer software are to be expressly stated in, or incorporated in, the contract.

   (e) This Notice shall be marked on any reproduction of this computer software, in whole or in part.

Contents

Preface

Chapter 1   Introduction

Chapter 2   Device Views

Chapter 3   Configuration Views

Chapter 4   Event and Alarm Messages

Chapter 5   Application View

Index

Figures

Chapter 1 — Introduction

Chapter 2 — Device Views

Chapter 3 — Configuration Views

Chapter 5 — Application View

Tables

Chapter 2 Device Views

Chapter 4 Event and Alarm Messages

Preface

Use this guide as a reference for the SPECTRUM management software that supports the ESX Devices described in Chapter 1. Before using this guide, you should be familiar with SPECTRUM's functions and navigational techniques as described in the ***Administrator's Reference*** and the ***Operator's Reference***.

What Is in This Guide

The following outlines the organization of this management module guide.

Chapter	Description
Chapter 1 *Introduction*	Describes the devices, the management module software, and model types.
Chapter 2 *Device Views*	Describes the Device views representing the devices.
Chapter 3 *Configuration Views*	Describes the Configuration views for the devices and the network management information provided by the views.
Chapter 4 *Event and Alarm Messages*	Lists and explains the event and alarm messages generated in the Event Log or Alarm Manager for the device model types.
Chapter 5 *Application View*	Describes the Application view and application-specific information for the devices.

Conventions

This guide uses the following conventions:

- Menu selections and buttons referenced in text appear in **bold**; for example, **Configuration** or **Detail**.

- Button names appear in shadowed boxes when introducing paragraphs describing their use; for example:

  | Help |

- Menu navigation appears in order of selection; for example, **Icon Subviews** -> **Utilities** -> **Application**.

- Referenced chapter titles and section headings appear in *italics*.

- Referenced documents appear in ***bold italics***.

- References in blue are hypertext links for online documents.

- The ESX Devices are referred to as the "devices."

Related SPECTRUM Documentation

It is important when using this guide that you have a clear understanding of SPECTRUM functionality and navigation techniques as described in the following recommended documentation:

Operator's Reference

Administrator's Reference

Report Generator User's Guide

Application View Reference

Getting Started with SPECTRUM 4.0 for Operators

Getting Started with SPECTRUM 4.0 for Administrators

How to Manage Your Network with SPECTRUM

Routing Services Management Module Guide

SPECTRUM Portable Management Application Tools Guide

Other Related Documentation

Refer to the following documentation for more information on managing TCP/IP-based networks:

Martin, James, Chapman, Kathleen Kavanagh, Leben, Joe. ***Local Area Networks: Architectures and Implementations***, 2d ed. Englewood Cliffs, NJ: Prentice Hall, 1994.

Rose, Marshall T. ***The Simple Book: An Introduction to Management of TCP/IP-based Internets***. Englewood Cliffs, NJ: Prentice Hall, 1991.

Stallings, William. ***Data and Computer Communications***, 4th ed. New York: Macmillan Publishing Company, 1994.

Tanenbaum, Andrew S. ***Computer Networks***, 3d ed. Englewood Cliffs, NJ: Prentice Hall, 1996.

Introduction

What Is in This Chapter

This chapter covers the following topics:

- ESX Devices
- SPECTRUM Support
- Accessing SPECTRUM Views
- SPECTRUM Views Roadmap

ESX Devices

This management module manages Cabletron's ESXMIM Ethernet Switching Media Interface Module, ESXMIM-F2 Fiber-Optic Ethernet Switching Media Interface Module, and ESX-1320/1380 Ethernet Workgroup Switches.

The ESXMIM is a multi-function hub module that provides integrated bridging and fast packet switching capabilities to the MMAC hub. It provides five 10Base-T ports, one slot for a Bridge/Router Interface Module (BRIM), and one slot for an Ethernet Port Interface Module (EPIM).

The ESXMIM-F2 provides the same functionality as the ESXMIM but supports five dual ST fiber-optic ports, one BRIM interface, and one EPIM interface.

The ESX-1320/1380s are standalone devices that provide ESXMIM capabilities to workgroups and remote offices. The ESX-1320 provides 12 switched 10Base-T full duplexed ports and one BRIM slot. The ESX-1380 is identical except that it provides 12 switched 10Base-FL full duplexed fiber ports and one BRIM slot.

The BRIMs and EPIMs are optional. They transfer packets between different channels. However, unlike EPIMs, BRIMs bridge these packets from one transmission type to another (e.g., Ethernet to FDDI network backbones). Possible BRIMs are as follows:

- BRIM-F6: FDDI Dual Attached Station (DAS) connection
- BRIM-E6: Ethernet module with selectable media connections
- BRIM-T6: Token Ring connection
- BRIM-A6: Asynchronous Transfer Mode connection

SPECTRUM Model Types

This section describes the model types used in SPECTRUM to manage the devices, and it describes how to access the SPECTRUM views that provide the management information.

Model Types

The following model type names refer to the models used to specify attributes, actions, and associations for the devices in SPECTRUM:

- ESXMIM is used for the ESXMIM and ESXMIM-F2
- ESXW is used for the ESX-1320 and ESX-1380

When modeling a device, the following selections appear in the Select Model Type dialog box:

- BRtrCSIESXM for the ESXMIM and ESXMIM-F2
- BRtrCSIESXW for the ESX-1320 and ESX-1380

Refer to the ***Administrator's Reference*** for modeling instructions.

Accessing SPECTRUM Views

The Device icon provides access to SPECTRUM views that display device-specific information. Access these views using double-click zones (Figure 1-1) or Icon Subviews menus (Figure 1-2 and Figure 1-3).

To access the Icon Subviews menu, do the following:

1. Highlight the icon.

2. From the View menu, select **Icon Subviews** or click the applicable mouse button (middle or right). Refer to the ***Operator's Reference*** for information on configuring your mouse.

Figure 1-1. **Using Double-Click Zones to Access SPECTRUM Views**

Accesses the Configuration view;
refer to Chapter 3, *Configuration
Views.*

Accesses the Device Topology view;
refer to the ***Operator's Reference***.

Accesses the Device view; see
Chapter 2, *Device Views.*

Model Name

ESXMIM

Accesses the Performance view;
refer to the ***Operator's Reference***.

Accesses the Application view; see
Chapter 5, *Application View.*

Accesses the Configuration view; see
Chapter 3, *Configuration Views.*

Accesses the Device view; see
Chapter 2, *Device Views.*

Accesses the Performance view;
refer to the ***Operator's Reference.***

Model Name

ESXMIM

Accesses the Device Topology view;
refer to the ***Operator's Reference***.

Accesses the Application view; see
Chapter 5, *Application View.*

Figure 1-2.   Using the Icon Subviews Menu to Access SPECTRUM Views
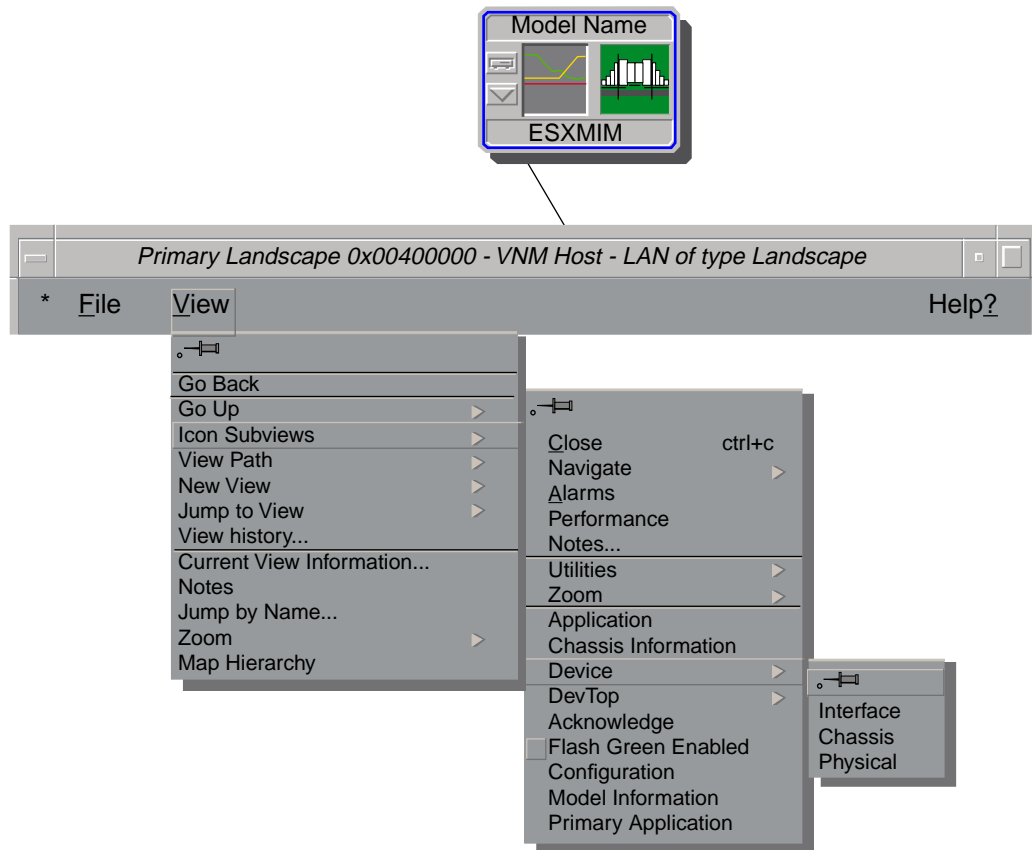
Figure 1-3.   Accessing Device-Specific Subviews
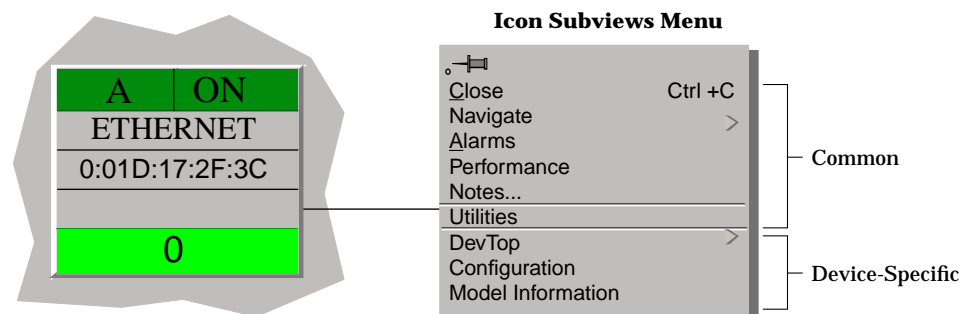
SPECTRUM Views Roadmap

Figure 1-4 shows a "roadmap" of the SPECTRUM views for the devices. These views are accessible from double-click zones (Figure 1-1) and Icon Subviews menus (Figure 1-2 and Figure 1-3).

Figure 1-4. **SPECTRUM Views Roadmap**
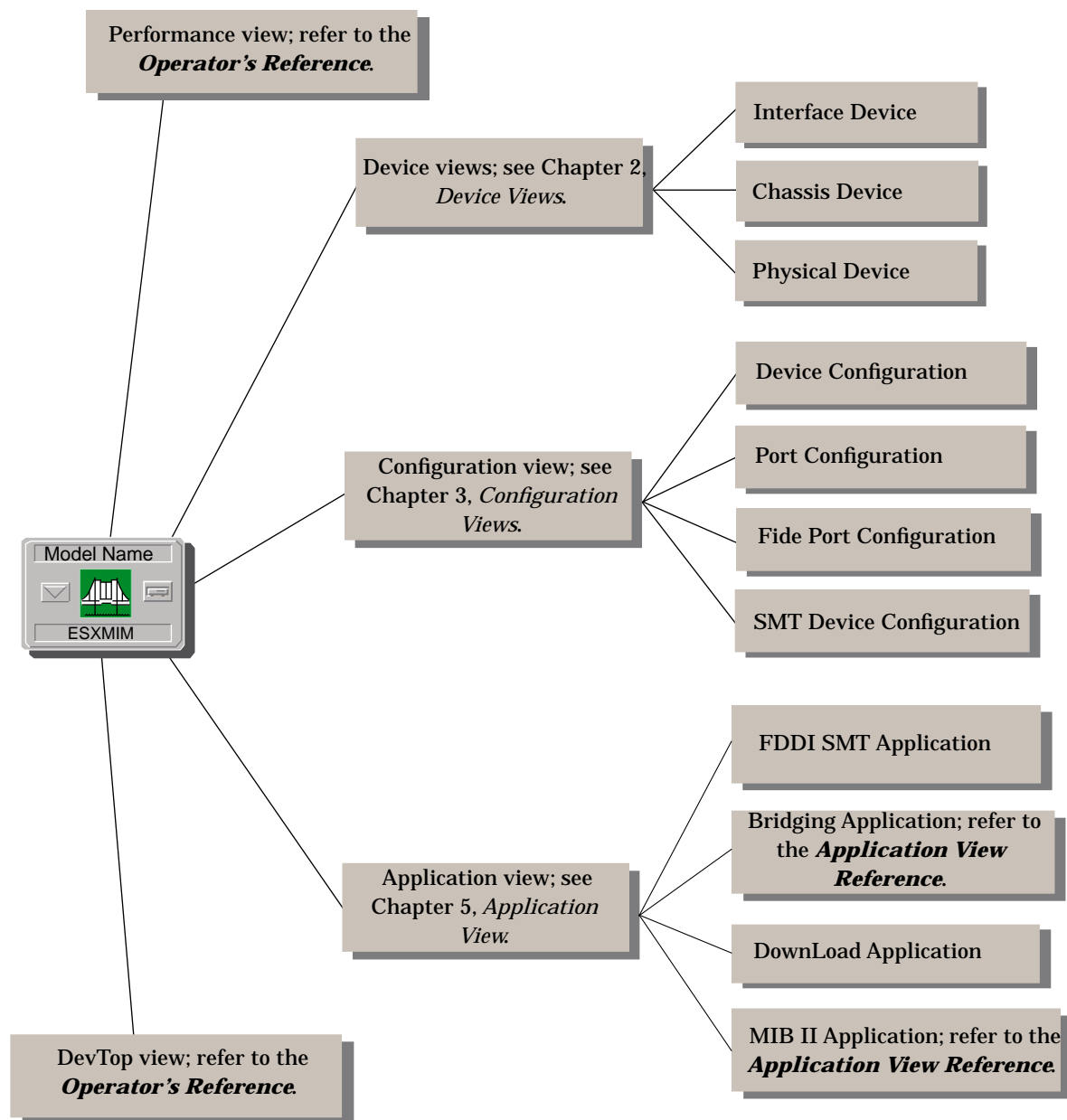
Chapter 2

Device Views

What Is in This Chapter

This chapter describes the following Device views and subviews for the devices:

- Interface Device view
- Chassis Device view
- Physical Device view

See Chapter 1 for information on accessing views and subviews.

Interface Device View

This view (Figure 2-1) provides dynamic configuration and performance information for each interface on a device. If the configuration changes, SPECTRUM modifies the Interface Device view after the next polling cycle to reflect the new configuration. This view also provides a Device icon that allows you to monitor the device's operation and access other device-specific views.

This section describes the Interface icons and Interface Options panel displayed in the Interface Device view. The number and type of Interface icons displayed on the Interface Device view depends on the device being viewed.

Figure 2-1.   Example of an Interface Device View
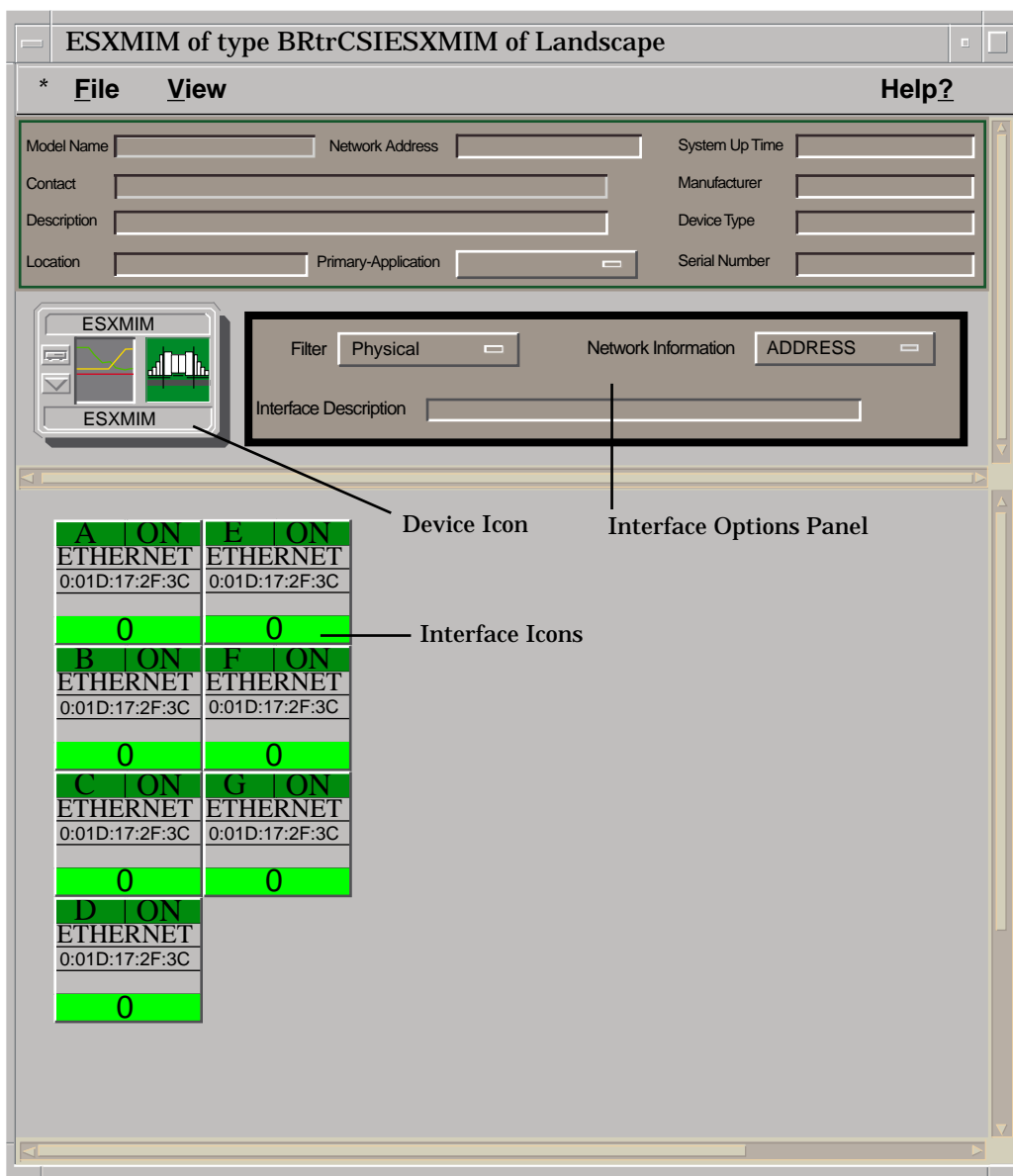
Interface Icons

These icons represent the interfaces or ports of a device. The icons identify the type of interface or port and provide statistical information. Figure 2-2 shows an example of an Interface icon, its Icon Subviews menu, and its labels/double-click zones.
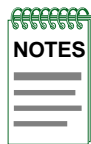
> **NOTES**
>
> The callouts (a through f) displayed in the graphic below illustrate the labels and, when available, the views to which they provide double-click access. For example, Administrative Status Label/Port Configuration-CSIIfPort View displays the administrative status of the interface and provides double-click access to the Port Configuration-CSIIfPort view.
>
> The menu displayed in the graphic is the Icon Subviews menu for that Interface icon.

Figure 2-2.   Example of an Interface Icon
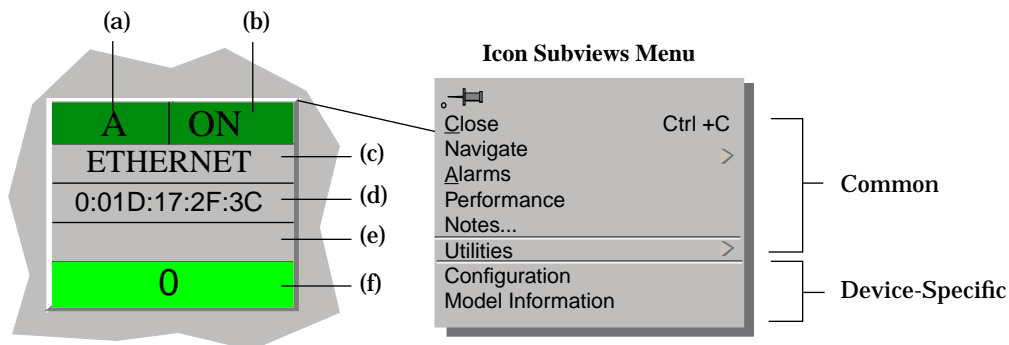
a.   Interface Label

b.   Administrative Status Label/Port Configuration-CSIIfPort View

c.   Interface Type Label

d.   MAC Address Label/CSI Interface Port Model Information View

e.   Network Information Label/Network Information Panel

f.   Gauge Label/Performance - CSIIfPort View

Interface Icon Subviews Menus

Table 2-1 describes the Interface Icon Subviews menu selections.

Table 2-1. **Icon Subviews Menu Selections**

Menu Selection	Description
Configuration	Opens the Port Configuration - CSIIfPort view described in Chapter 3, Configuration Views.
Model Information	Opens the Model Information view described in the ***Operator's Reference***.

Interface Label

This label displays the interface number.

Administrative Status Label

This label displays the status of this interface. Double-click this label to open the *Port Configuration-CSIIfPort View* described on Page 3-3.

Table 2-2 and Table 2-3 list the possible states relative to the application selected. The default application for this view is Physical (MIB-II). To select the application to be displayed (Physical or Bridging), click the **Filter** menu button in the Interface Options panel. The Filter menu button is described under *Interface Options Panel on Page 2-6.*

Table 2-2. **Administrative Status for the Physical or MIB II Application**

Color	Status	Description
Green	ON	Port is operational.
Yellow	OFF	Port is off.
Blue	TST	Port is in the test mode.

Table 2-3. **Administrative Status for the Bridging Application**

Color	Status	Description
Green	FWD	Bridge port is forwarding.
Blue	DIS	Port is disabled.
Magenta	LST	Bridge is in the listening mode.
Magenta	LRN	Bridge is in the learning mode

Table 2-3. **Administrative Status for the Bridging Application**

Color	Status	Description
Orange	BLK	Bridge port is in the blocking mode.
Red	BRK	Bridge port is broken.

Interface Type Label

This label displays the interface type, for example, Ethernet, FDDI, etc.

MAC Address Label

This label displays the MAC address of the device interface. Double-click this label to open the CSI Interface Port Model Information view described in the ***Operator's Reference***.

Network Information Label

This label displays user-selectable network information (Address, Name, or Mask). The default is Address. Double-click this label to open the Network Information Panel.

To change this label's display, use the Interface Options Panel described below, or do the following:

1.   Double-click the label to open the Network Information Panel.

2.   Click the network information entry you wish to display.

3.   Click **OK**.

Gauge Label

This label displays the performance statistic determined by the Gauge Control Panel for this interface. (Refer to the *Gauge Control Panel* described below for more information.) Double-click this label to open the Performance-CSIIfPort view described in the ***Operator's Reference***.

Interface Options Panel

This area of the Interface Device view allows you to modify the presentation of a highlighted Interface icon. Double-click a non-text area of this panel to open the Gauge Control Panel, described below. The Interface Options panel provides the following information:

Filter
Allows you to select the application to be displayed by the Interface icons. You can leave the default, which is Physical (MIB II), or select Bridging. You can also select other applications (purchased separately) such as IP routing if the SPECTRUM Routing Services Management Module is loaded. For more information, refer to the ***Routing Services Management Module Guide***.

Network Information
Allows you to select the type of information displayed in the Network Information label of the highlighted Interface icon. Possible selections are ADDRESS, NAME, or MASK.

Interface Description
Provides a description of the highlighted interface. If no interface is highlighted, this field is empty.

Gauge Control Panel

This panel (Figure 2-3) allows you to change the type of statistical information displayed on the Gauge label of the Interface icon. To access the Gauge Control Panel, double-click the background of the Interface Options panel or do the following:

1. Highlight the Interface Options panel.

2. From the View menu, select **Icon Subviews** -> **Gauge Control Panel**.

Figure 2-3.   **Gauge Control Panel**
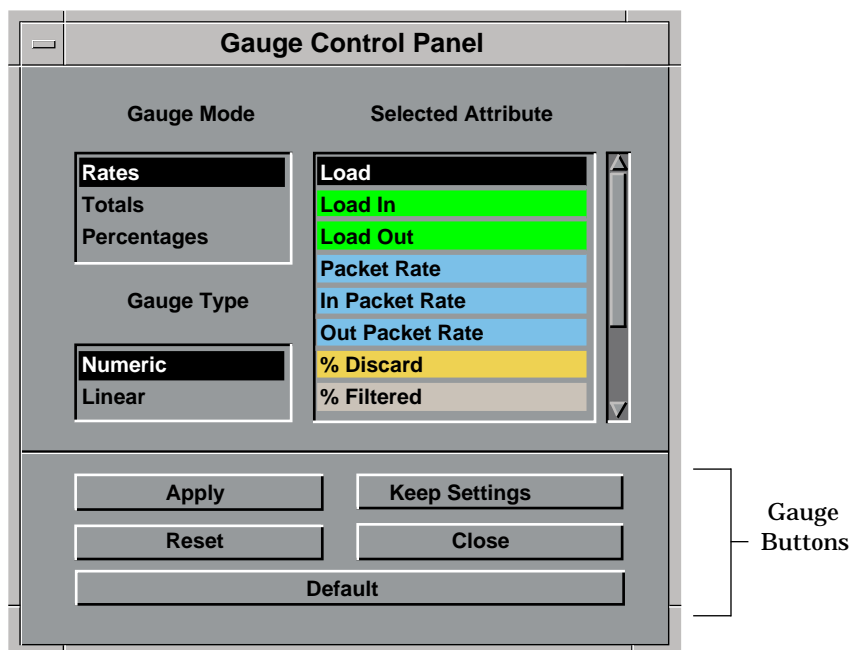
The Gauge Control Panel provides the following:

- Gauge Mode panel
- Selected Attribute panel
- Gauge Type panel
- Gauge Buttons

Gauge Mode
This panel allows you to select the type of information shown on the Gauge label of the Interface icon: Totals, Rates, or Percentages. The Percentages selection displays the percentage of the selected interface compared to the rest of the interfaces.

The color displayed on the Gauge label depends upon the particular mode and statistical attribute selected. Table 2-4 and Table 2-5 provide a list of attributes and their corresponding colors for the Totals mode and Rates mode, respectively.

Table 2-4.   **Totals Gauge Mode: Attributes and Corresponding Color**

Selected Attribute	Color
Errors	Black
In Packets	Blue
Out Packets	Blue
In Octets	Green
Out Octets	Green
Discards	Tan
Forwarded	Purple
Host Bound	Yellow
Transmitted	White
Filtered	Gray

Table 2-5.   **Rates Gauge Mode: Attributes and Corresponding Color**

Selected Attribute	Color
Load	Black
Load In	Green
Load Out	Green
Packet Rate	Blue
In Packet Rate	Blue
Out Packet Rate	Blue
% Discard	Tan
% Filtered	Gray
% Forwarded	Violet
% Host Bound	Yellow
% Error	Orange
% Transmitted	White

Selected Attribute
This panel allows you to select the statistical attribute displayed on the
Interface icon's Gauge label. The label changes color to reflect the attribute
selected.

Gauge Type
This panel allows you to select either a numeric or linear display on the Gauge
label.

Gauge Buttons
The following describes the Gauge buttons:

Apply

Applies the current settings to the Gauge label temporarily but does not save
the settings.

Reset

Returns the settings to the previously saved values.

Keep Settings

Saves the current settings while SpectroGRAPH is running. Settings return to
default when you restart SpectroGRAPH.

Close

Closes the Gauge Control Panel.

Default

Returns the settings to the SPECTRUM default.

Chassis Device View

This section describes the information available from the Chassis Device view,
which provides access to detailed information about the chassis, each module,
the applications, and the ports. Figure 2-4 and Figure 2-5 show examples of
the Chassis Device view for the ESXMIM and ESX-1320/80.

Figure 2-4.   Example of an ESXMIM Chassis Device View
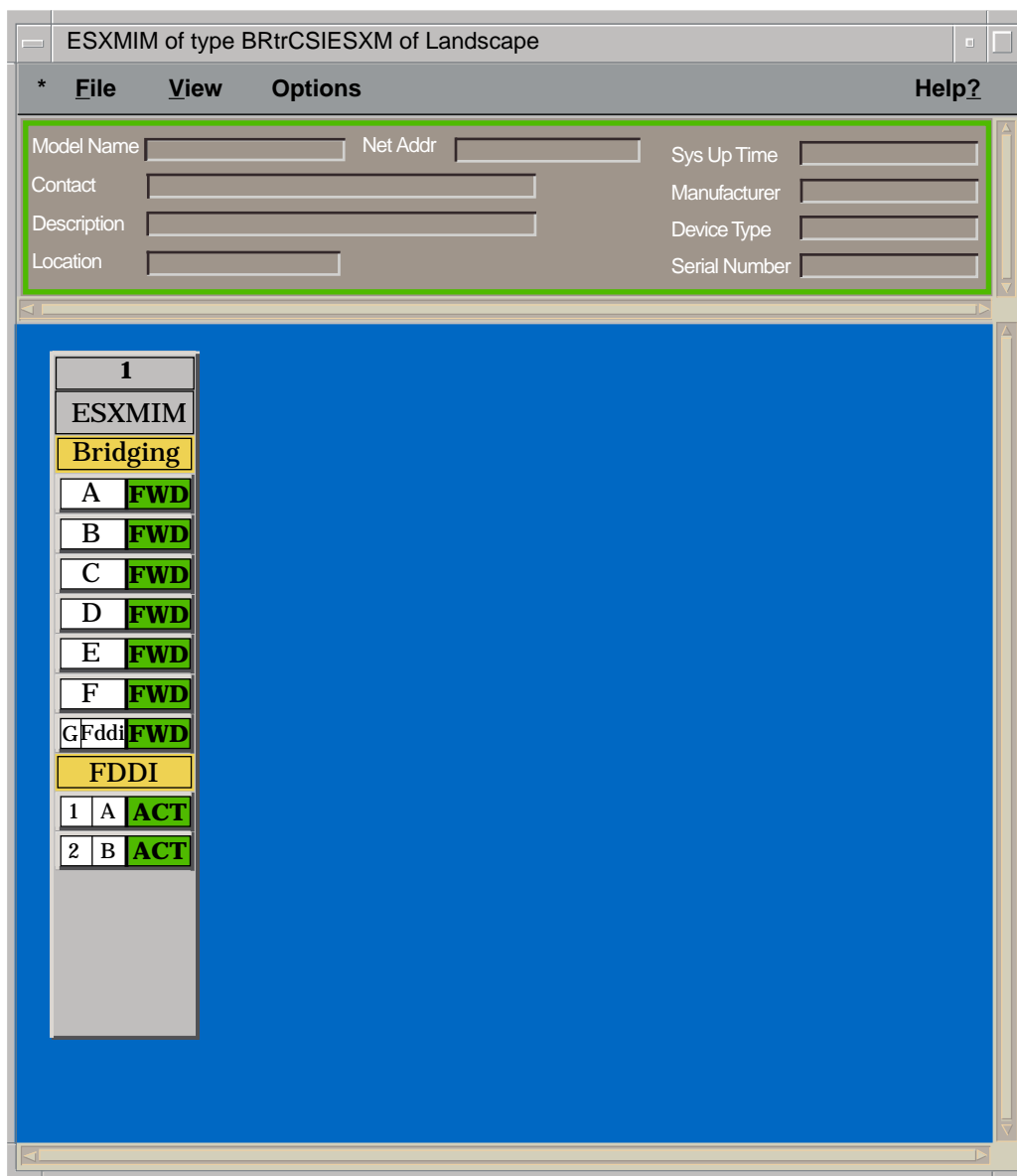
Figure 2-5.   Example of an ESX-1320/80 Chassis Device View
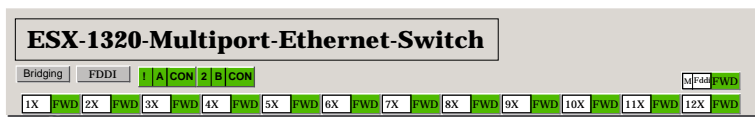
Chassis Module Icon

This icon is a logical representation of the physical module, its location in the Chassis, and its front panel interfaces or ports. This section describes the information available from the Chassis Module icon. Figure 2-6 shows an example of a Chassis Module icon, its labels and, when applicable, the views to which the labels provide double-click access. The information listed within blocks represent the Icon Subviews menu selections.

Figure 2-6.   **Chassis Module Icons, Labels, and Menu Selections**
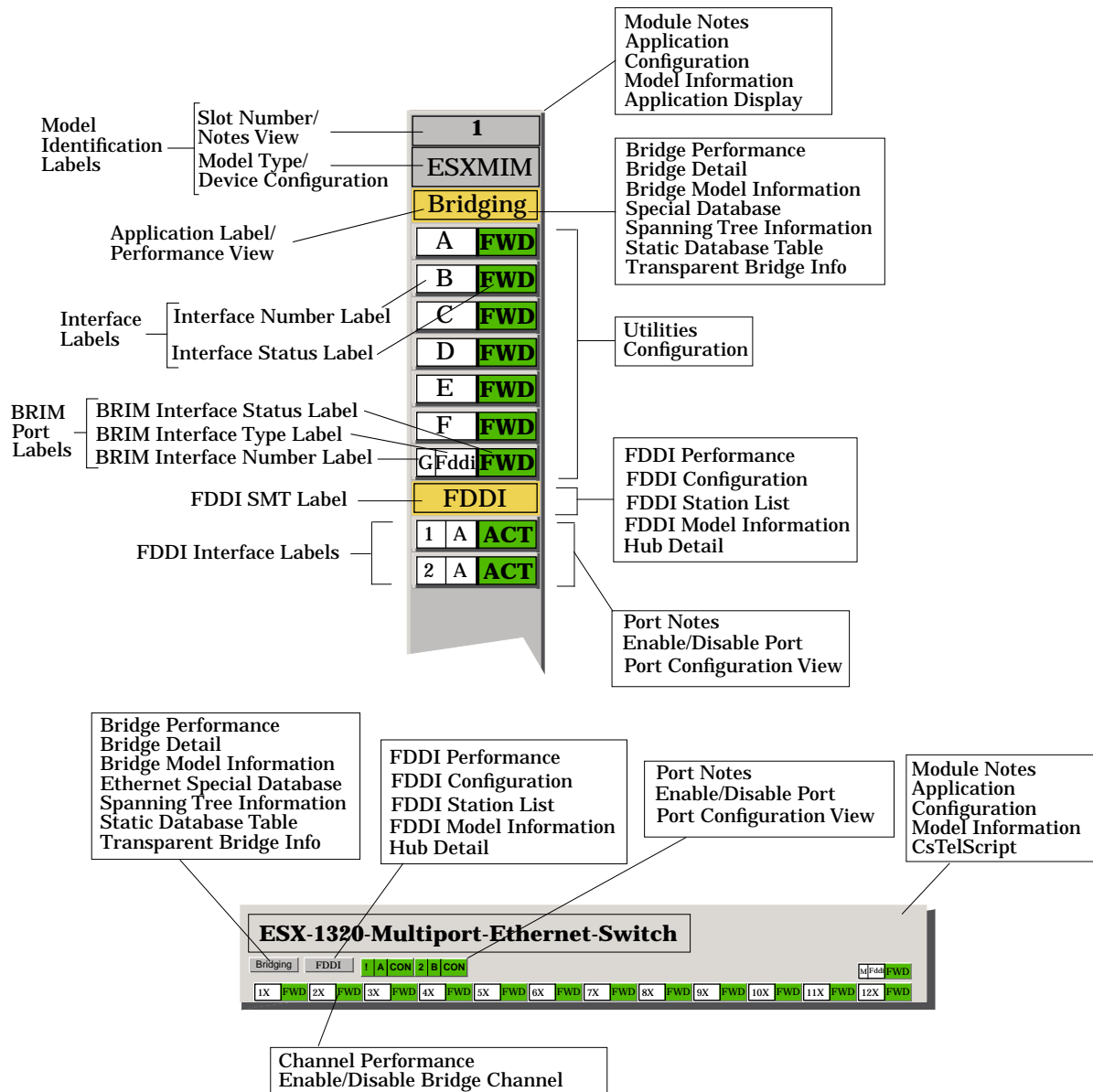
Model Identification Labels

These labels provide the following information.

Slot Number
Identifies the module's location in the chassis. Double-click this label to open the Notes view.

Model Type
Identifies the type of module being displayed. Double-click this label to open the *Device Configuration View* described on Page 3-2.

Chassis Module Icon Subviews Menu

Table 2-6 describes each of the device-specific Icon Subviews menu selections available for this device. See Chapter 1 for information on accessing device-specific subviews.

Table 2-6. **Module Icon Subviews Menu**

Menu Selection	Description
Module Notes	Opens the Notes view described in the ***Operator's Reference***.
Application	Opens the Application view described in Chapter 5.
Configuration	Opens the *Device Configuration View* described on Page 3-2.
Model Information	Opens the Model Information view described in the ***Operator's Reference***.
Application Display	Allows you to select the Primary Application, either Bridging or Physical.

Application Label

This label displays the application selected and provides access to its Icon Subviews menu. The application selected determines the information displayed and the menu selections available. The default application for this view is Bridging.

To select the application, highlight the Chassis Module icon and select **View** > **Icon Subviews** > **Application Display**.

Double-click the Application label to open the Performance view described in the ***Operator's Reference***.

Table 2-7 describes the Bridging Application Icon Subviews menu selections. There are no specific Icon Subviews menu selections for the Physical Application.

Table 2-7. **Bridging Application Icon Subviews Menu**

Menu Selection	Description
Bridge Performance	Opens the Bridge Performance view described in the ***Operator's Reference***.
Bridge Detail	Opens the Bridge Detail view described in the ***Application View Reference***.
Bridge Model Information	Opens the Model Information view described in the ***Operator's Reference***.
Special Database	Opens the Bridge Ethernet Special Database Tables view described in the ***Application View Reference***.
Spanning Tree Information	Opens the Spanning Tree Information view described in the ***Application View Reference***.
Static Database Table	Opens the Static Database Table view described in the ***Application View Reference***.
Transparent Bridge Info	Opens the Transparent Bridge Information view described in the ***Application View Reference***.

Interface Labels

These labels (Figure 2-6 on Page 2-11) represent the interfaces located on the front panel of the device and provide access to the Icon Subviews menu for the interfaces. Two information labels are displayed: an Interface Number label and an Interface Status label, which are described below. The device-specific Icon Subviews menu selection for the Interface label is **Configuration**. It opens the Configuration dialog box, which allows you to enable or disable the selected port.

Interface Number Label
This label uniquely identifies the interface represented.

Interface Status Label
This label indicates the port activity status. Table 2-8 and Table 2-9 describe the possible states relative to the application selected. See *Application Label* described on Page 2-12 for information on selecting the application to be displayed.

Table 2-8.   **Interface Status for the Bridging Application**

Color	Status	Description
Green	FWD	Port is forwarding network traffic.
Blue	DIS	Port is disabled.
Magenta	LST	Port is in the listening mode.
Magenta	LRN	Port is in the learning mode.
Blue	SBY	Port is in the standby mode.
Orange	BLK	Port is in the blocking mode.
Red	BRK	Port is broken.
Blue	UNK	The status is unknown.

Table 2-9.   **Interface Status for the Physical or MIB II Application**

Color	Status	Description
Green	ON	Port is operational.
Blue	OFF	Port is off.
Yellow	TST	Port is in the test mode.

BRIM Port Labels

These labels (Figure 2-6 on Page 2-11) represent the FDDI BRIM installed in the ESXMIM. They provide access to the Icon Subviews menu for the interface. This label displays three information labels: a BRIM Interface Number label, BRIM Interface Type label, and BRIM Interface Status label. The menu selection for these labels is **Configuration**, which opens the Configuration dialog box that allows you to enable or disable the port.

BRIM Interface Number Label
This label shows the interface number for the FDDI BRIM.

BRIM Interface Type Label
This label shows the interface type (FDDI).

BRIM Interface Status Label
This label indicates the port activity status of the FDDI BRIM. Table 2-8 and Table 2-9 show the possible states relative to the application selected.

FDDI SMT Label

This label shows the application type and provides access to FDDI station management information through its Icon Subviews menu, which provides the selections listed in Table 2-10.

Table 2-10. **FDDI Icon Subviews Menu Selections**

Menu Selection	Description
FDDI Performance	Opens the FDDI Performance view described in the **Operator's Reference**.
FDDI Configuration	Opens the SMT Device Configuration view described in the **Applications View Reference**.
FDDI Station List	Opens the FDDI Station List view described in the **Applications View Reference**.
FDDI Model Information	Opens the SMT Model Information view described in the **Operator's Reference**.
Hub Detail	Opens the FddiSMT Detail View described in the **Applications View Reference**..

FDDI Interface Labels

FDDI has two ring-in/ring-out ports that are represented by the labels shown in Figure 2-6 on Page 2-11. These labels provide access to the Icon Subviews menu selections listed in Table 2-11. The ring-in/ring-out port status label color representations are listed in Table 2-12.

Table 2-11. **FDDI Port Icon Subview Menu Selections**

Menu Selection	Description
Port Notes	Opens the Ports Notes view described in the **Operator's Reference**.
Enable/Disable Port	Opens the Enable/Disable Port view, which allows you to enable and disable the port.
Port Configuration View	Opens the *FDDI Port Configuration View* described on Page 3-3.

Table 2-12.   **FDDI Port Status and Related Colors**

FDDI Port Status	Color
ACT (active)	Green
DIS (disabled)	Blue
CON (connecting)	Yellow
SBY (standby)	Red

Physical Device View

This view shows a static image of the device. Figure 2-7 and Figure 2-8 show examples of the Physical Device views for the ESXMIM and ESX-1320.

Figure 2-**7.** **ESXMIM Physical Device View**
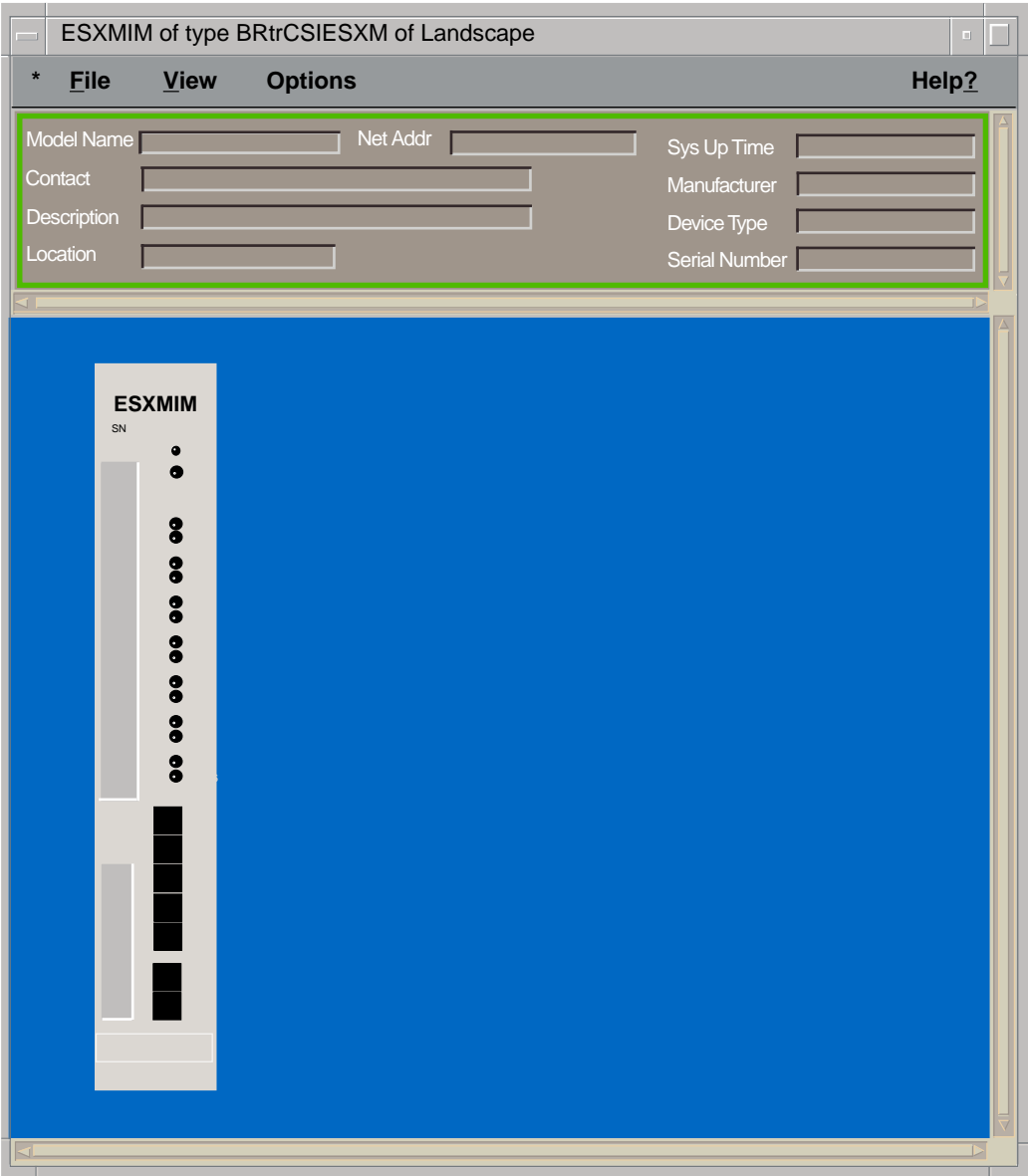
Figure 2-8.   **ESX-1320 Physical Device View**
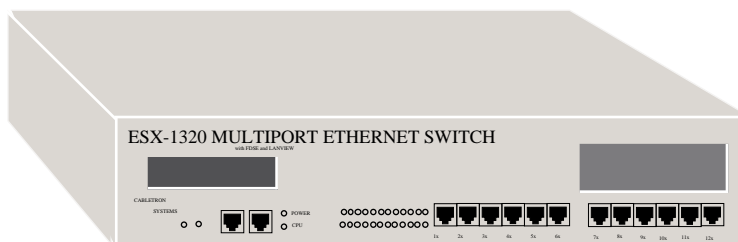
Configuration Views

This chapter provides descriptions of the configuration views that are available for the ESX Devices.

What Is in This Chapter

The Configuration views allow you to access device-specific configuration information. This management module supports the following configuration views:

- Device Configuration view
- Port Configuration - CSIIfPort view
- FDDI Port Configuration view
- SMT Device Configuration view described in the ***Application View Reference***

Device Configuration View

This view provides information on the configuration and operating status of the devices and allows you to change the network connections. It provides three fields as described below.

Contact Status
Indicates whether a connection with the device has been established.

Firmware Revision
The firmware revision for the device.

Hardware Revision
The hardware revision for the device.

This view also provides buttons (**Component Table**, **Download Application**, **Trap Table**, and **Date/Time**) that access SPMA applications that allow you to configure the devices. For details on the views accessible from these buttons, refer to the ***SPECTRUM Portable Management Application Tools Guide***.

Interface Configuration Table

This table provides the following configuration information for each interface or port.

Number of Interfaces
The number of interfaces or ports available for the devices.

Index
The interface or port number.

Type
The type of hardware interface or port, for example, Ethernet, FDDI, etc.

Phy Address
The Ethernet (MAC) address of the interface or port.

Max Frame Size
The maximum frame size for the interface or port (e.g., 4500).

Oper Status
The current operational state of this interface or port (Up, Down, or Testing).

Port Configuration-CSIIfPort View

This view provides information on the configuration and operating status of this device's interfaces or ports. To access the Port Configuration-CSIIf Port view, do the following:

1.   Within the Interface Device view, highlight the Interface icon.

2.   From the Icon Subviews menu, select **Configuration**.

This view provides the following fields:

Interface Index
The numerical value identifying the interface or port.

Interface Type
The type of interface.

Operation Status
The current operating status of the interface or port. Possible values are **On** (enabled), **Off** (disabled), and **Test**.

Admin Status
Allows you to set the administrative state of the interface or port. Possible values are **On** (enabled), **Off** (disabled), and **Test**.

IF Description
Describes the interface or port.

FDDI Port Configuration View

This view provides information concerning the configuration of the FDDI port. To access this view, highlight the FDDI Interface icon on the Chassis Device view and select **Port Configuration View** from the Icon Subviews menu.

Port Configuration View Banner

This view displays the following information:

Model Name
The FDDI SMT chassis model name.

Network Address
The IP address of the FDDI SMT.

SMT.Port
The number to the left of the decimal represents the FDS SMT number and the number to the right represents the port index.

Port Management

The Port Management section of the FDDI Port Configuration View provides the following information:

Port Action
Allows you to enable and disable the port. The state returns to **Other** once the port has been enabled or disabled.

Port State
The status of this port. Possible states are: **Disabled**, **Connecting**, **Standby**, and **Active**.

Port Type
The type of port. Possible port types are: **A_Port**, **B_Port**, **Slave**, or **Master**.

Link Error Rate Estimate
The link error rate estimate is a cumulative long-term average of the bit error rate, which represents the quality of the physical link. The link error rate estimate is computed when the port is connected and every 10 seconds thereafter. It ranges from 10^{-4} to 10^{-15} and is reported as a whole integer representing the exponent. For example, if the port's link error rate estimate is computed to be 10^{-5}, the value reported in this field would be 5, which represents an actual rate of 1,250 bit errors per second. A lower link error rate estimate indicates a higher bit error rate as shown in Figure 3-1.

Figure 3-1.   **Link Error Rate Estimate**

Reported Link Error Rate Estimate (n)
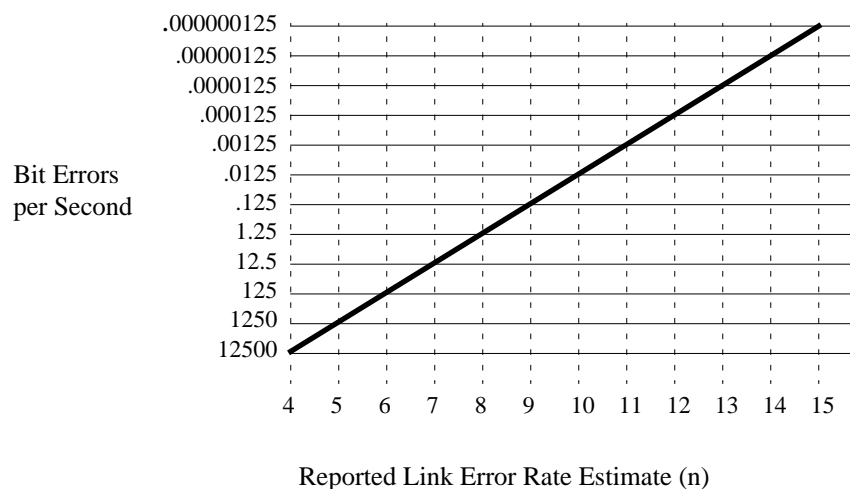
Link Error Monitor Count
The aggregate link error monitor count. This count is set to zero on station power up and increments each time the port's link error monitor detects an error. An increasing link error monitor count usually indicates a problem with the connectors or the cable between this port and the node.

Link Error Rate Cutoff
The link error rate threshold at which a link connection is flagged as faulty and the port disabled by SMT. The default link error rate cutoff threshold is 7, which represents 12.5 bit errors per second (Figure 3-1). This value can be changed.

Link Error Rate Alarm
The link error rate threshold which, if exceeded, generates an alarm for the port. The default link error rate alarm threshold is 8, which represents 1.25 bit errors per second (Figure 3-1). This value can be changed.

Link Error Monitor Reject Count
The link error monitor count of the times the link has been rejected.

Event and Alarm Messages

What Is in This Chapter

This chapter lists the types of events and alarms generated by the devices and provides any probable cause messages corresponding to these alarms.

Events and Alarms

Table 4-1 lists the SPECTRUM database directory paths (in bold) and the messages displayed for the Event Log and Alarm Manager, when applicable.

Table 4-1. **Device Events and Alarms**

CsEvFormat/Event00010306 {d "%w- %d %m-, %Y - %T"} A(n) {t} device, named {m}, has been cold started. (event [{e}])	No Probable cause message.
CsEvFormat/Event00010307 {d "%w- %d %m-, %Y - %T"} A(n) {t} device, named {m} has been warm started. (event [{e}])	No Probable cause message.
CsEvFormat/Event00010308 {d "%w- %d %m-, %Y - %T"} A(n) {t} device, named {m}, has detected a communication Link Down. (event [{e}])	**CsPCause/Prob00010308** Communication link is down.

Table 4-1. **Device Events and Alarms**

CsEvFormat/Event00010309 {d "%w- %d %m-, %Y - %T"} A(n) {t} device, named {m}, has detected a communication Link Up. (event [{e}])	No Probable cause message.
CsEvFormat/Event0001030a {d "%w- %d %m-, %Y - %T"} A(n) {t} device, named {m}, has detected an Authentication Failure. (event [{e}])	**CsPCause/Prob0001030a** Authorization failure. Other user is trying to connect to device with an invalid community string.
CsEvFormat/Event0001030b {d "%w- %d %m-, %Y - %T"} A(n) {t} device, named {m}, has detected an EGP Neighbor Loss. EGP Neighbor IP address is {O 1}. (event [{e}])	**CsPCause/Prob0001030b** Lost contact with EGP neighbor.
CsEvFormat/Event000d01a0 {d "%w- %d %m-, %Y - %T"} A Port Interface Module has been inserted into port {I 3} of interface {I 1} on {m} ({t}). (event [{e}])	**CsPCause/Prob000d01a0** A Port Interface Module has been physically inserted.
CsEvFormat/Event000d01a1 {d "%w- %d %m-, %Y - %T"} A Port Interface Module has been removed from port {I 3} of interface {I 1} on {m} ({t}). (event [{e}])	**CsPCause/Prob000d01a1** A Port Interface Module has been physically removed.
CsEvFormat/Event000d01a2 {d "%w- %d %m-, %Y - %T"} Network configuration change reported by {m} ({t}). Device linked to port {I 3} on interface {I 1}. (event [{e}])	**CsPCause/Prob000d01a2** A device supporting link integrity, fiber optic or twisted pair, has made a valid connection (link) to this port.
CsEvFormat/Event000d01a3 {d "%w- %d %m-, %Y - %T"} Port {I 3} on interface {I 1} of {m} ({t}), has unsegmented. (event [{e}])	**CsPCause/Prob000d01a3** A device previously linked with this port has been removed, powered down, or the cable segment has a fault.
CsEvFormat/Event000d0351 {d "%w- %d %m-, %Y - %T"} Front panel redundant port {I 1} has been activated by device {m} of type {t}. (event [{e}])	**CsPCause/Prob000d0351** A new port has been activated for the front panel redundant circuit. This does NOT indicate this port is usable, but is being tested.

Table 4-1.   **Device Events and Alarms**

CsEvFormat/Event000d0001	CsPCause/Prob000d0001
{d "%w- %d %m-, %Y - %T"} {m} of type {t} has reported a root change (event [{e}]).	This bridge has become the new root of the Spanning Tree.
CsEvFormat/Event000d0002	**CsPCause/Prob000d0002**
{d "%w- %d %m-, %Y - %T"} {m} of type {t} has reported a network topology change (event [{e}]).	A port has transitioned from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state.
CsEvFormat/Event000d0101	**CsPCause/Prob000d0101**
{d "%w- %d %m-, %Y - %T"} Port {I 3} on module in slot {I 1} of {m} ({t}), has segmented. (event [{e}])	The port has made 32 consecutive attempts to transmit and which resulted in a collision each time or the port collision detector was turned on for longer than 2.4 milliseconds. Either of these collision occurrences are caused by a cabling problem of extremely high rates of traffic on the segment the port is attached to.
CsEvFormat/Event000d0102	**CsPCause/Prob000d0102**
{d "%w- %d %m-, %Y - %T"} Port {I 3} on module in slot {I 1} of {m} ({t}), has unsegmented. (event [{e}])	The port has transmitted or received a valid packet. This can occur when a cable or termination fault has been corrected. Unsegmenting also can occur on a port that previously was not in use.
CsEvFormat/Event000d0103	**CsPCause/Prob000d0103**
{d "%w- %d %m-, %Y - %T"} Network configuration change reported by {m} ({t}). Device linked to port {I 3} on module in slot {I 1}. (event [{e}])	A device supporting link integrity, fiber optic or twisted pair, has made a valid connection (link) to this port.
CsEvFormat/Event000d0104	**CsPCause/Prob000d0104**
{d "%w- %d %m-, %Y - %T"} Network configuration change reported by {m} ({t}). Device previously linked to port {I 3} on module in slot {I 1} has ceased to transmit link integrity pulse. (event [{e}])	A device previously linked with this port has been removed, powered down, or the cable segment has a fault.
CsEvFormat/Event000d0105	**CsPCause/Prob000d0105**
{d "%w- %d %m-, %Y - %T"} New source address {X 5}, is detected on {m} ({t}), port {I 3} of module in slot {I 1}. (event [{e}])	A device, previously linked or not, has transmitted a packet that was received on this port. The device is either new or has been powered up but not transmitted a packet with the aging time period.

Table 4-**1.** **Device Events and Alarms**

CsEvFormat/Event000d0106	CsPCause/Prob000d0106
{d "%w- %d %m-, %Y - %T"} Source address {X 5}, has timed out on port {I 3} of the module in slot {I 1} of {m} ({t}). (event [{e}])	A device linked or not linked to this port has not transmitted a packet during the aging time period, and has been removed from the source address table of the device.
CsEvFormat/Event000d0107	**CsPCause/Prob000d0107**
{d "%w- %d %m-, %Y - %T"} Device configuration change reported by {m} ({t}). The module in slot {I 1} has been removed. (event [{e}])	A module within this hub has been removed or has failed.
CsEvFormat/Event000d0108	**CsPCause/Prob000d0108**
{d "%w- %d %m-, %Y - %T"} Device configuration change reported by {m} ({t}), An (EPIM) has been inserted into slot {I 1} of the MMAC. (event [{e}])	A module has been inserted into this hub.
CsEvFormat/Event000d0109	**CsPCause/Prob000d0109**
{d "%w- %d %m-, %Y - %T"} Network configuration change reported by {m} ({t}). Port {I 3} in slot {I 1} has failed redundancy polling and has switched to a backup port. (event [{e}])	The polled device(s) in the redundant circuit polling list have failed to respond. The device(s) have failed, been powered down or a cable fault from the active port to the polled device has occurred. Check the retry count as it may need to be adjusted on a busy network segment. Normal collision occurrences may occur causing the poll packet to not reach it's destination.
CsEvFormat/Event000d010a	**CsPCause/Prob000d010a**
{d "%w- %d %m-, %Y - %T"} Network configuration change reported by {m} ({t}). Port {I 3} in slot {I 1} has now become active as the result of a redundancy poll failure. (event [{e}])	The polled device has been communicated with via a backup port and the port is now active. The other ports in this redundant circuit are now designated as backup and are turned off to prevent data loops on the network.
CsEvFormat/Event000d010b	**CsPCause/Prob000d010b**
{d "%w- %d %m-, %Y - %T"} Redundancy diagnostics of {m} ({t}), indicate that the redundant link for module {I 1}, port {I 3} has failed. (event [{e}])	The cable segment connected to the port has a cable fault. This should be checked for continuity as soon as possible in case the other ports in this redundant circuit fail and this port is needed.

Table 4-1.   **Device Events and Alarms**

CsEvFormat/Event000d010f	CsPCause/Prob000d010f
{d "%w- %d %m-, %Y - %T"} User defined traffic threshold - {I 1} packets within {I 3} seconds, exceeded on module {I 5} of {m} ({t}). (event [{e}])	The packet rate on this module has exceeded user defined limits. The device(s) attached to this module may have an application which requires a large amount of network bandwidth. If the application requires a large amount of bandwidth, a bridge or router could be used to logically separate various network segments. Use port level thresholds to further troubleshoot to a device level.
CsEvFormat/Event000d0110	**CsPCause/Prob000d0110**
{d "%w- %d %m-, %Y - %T"} Error threshold exceeded. An error threshold, of {I 1}% of total packets in {I 5} seconds, exceeded on module in slot {I 7}. (event [{e}])	This threshold will indicate that a malfunctioning device is present on this module or that a cable fault exists. A port level threshold should be set to further troubleshoot to the offending node.
CsEvFormat/Event000d0111	**CsPCause/Prob000d0111**
{d "%w- %d %m-, %Y - %T"} Collision threshold exceeded. The number of collisins per total packets within the time base of {I 3} seconds has been exceeded on the module in slot {I 5} of {m} ({t}). (event [{e}])	Collisions are caused by many nodes contending for the network or cabling faults. Use port level thresholds to further troubleshoot to a device level.
CsEvFormat/Event000d0112	**CsPCause/Prob000d0112**
{d "%w- %d %m-, %Y - %T"} Traffic threshold, {I 1} packets per {I 3} seconds, exceeded on port {I 7} on module in slot {I 5} of {m} ({t}). (event [{e}])	The device(s) attached to this port may have an application which requires a large amount of network bandwidth. If the application requires a large amount of bandwidth, a bridge or router could be used to logically separate various network segments.
CsEvFormat/Event000d0113	**CsPCause/Prob000d0113**
{d "%w- %d %m-, %Y - %T"} Error threshold exceeded. An error threshold, of {I 1}% of total packets in {I 5} seconds, exceeded on port {I 9} on module in slot {I 7} of {m} ({t}). (event [{e}])	The device(s) attached to this port could have a hardware failure where it transmits invalid packets, or the cable segment attached to this port may have a problem. Check cable for loose connection or continuity problems.

Table 4-1. **Device Events and Alarms**

CsEvFormat/Event000d0114	CsPCause/Prob000d0114
{d "%w- %d %m-, %Y - %T"} Collision threshold exceeded. The number of collisins per total packets within the time base of {I 3} seconds has been exceeded on port {I 7} on module in slot {I 5} of {m} ({t}). (event [{e}])	The device(s) attached to this port may have an adapter card problem which causes them to transmit without regarding network availability, or a cable problem may exist. Check adapter card and cable for loose connections, termination problems, or improper pinouts.
CsEvFormat/Event000d0115	**CsPCause/Prob000d0115**
{d "%w- %d %m-, %Y - %T"} Port Topology type changed. Port {I 3} of module in slot {I 1} has changed from {T PrtTopoStatus 5} port on {m} ({t}). (event [{e}])	The number of addresses in the source address table has changed. If three or more addresses are learned on a port for one aging time period, the port is designated as a trunk port. A port connecting two hubs or a coax segment with multiple taps are examples of trunk ports. If a port has one address in the source address table for one aging time, the port is designated as a station port. An example of a station port would be a twisted pair "home run" to a PC.
CsEvFormat/Event000d0117	**CsPCause/Prob000d0117**
{d "%w- %d %m-, %Y - %T"} Port security violation has occurred, MAC address {X 5} has been detected on port {I 3} of module in slot {I 1} of {m} ({t}). (event [{e}])	This event is only generated when the hub has port locking enabled. When a hub is locked, the source MAC addresses are learned on each port. When a port detects an attached device has changed its address, the device will note that the new address is not in the source address table. This will disable and lock the port, which then transmits this trap. This trap would be generated if an adapter were replaced or if an intruder attempted to access the network.
CsEvFormat/Event000d0118	**CsPCause/Prob000d0118**
{d "%w- %d %m-, %Y - %T"} Port violation reset, port {I 3} of module in slot {I 1} of {m} ({t}). (event [{e}])	The network administrator has located the offending device that caused the port violation, and has re-enabled the port for use by the original network address for that port.

Table 4-1. **Device Events and Alarms**

CsEvFormat/Event000d0119	CsPCause/Prob000d0119
{d "%w- %d %m-, %Y - %T"} Environment Temperature Warm condition for module in slot {I 1} reported by {m} ({t}). (event [{e}])	The module may be defective or a fan has failed in the chassis. Check the alarm log for this device for any fan alarms.
CsEvFormat/Event000d011a	**CsPCause/Prob000d011a**
{d "%w- %d %m-, %Y - %T"} Environment Temperature Hot condition for module in slot {I 1} reported by {m} ({t}). (event [{e}])	A module may be defective or a fan has failed in the chassis. This alarm indicates a serious heat condition and should be addressed immediately.
CsEvFormat/Event000d011b	**CsPCause/Prob000d011b**
{d "%w- %d %m-, %Y - %T"} Environment Voltage Low condition has been detected by power supply in slot {I 1} of {m} ({t}). (event [{e}])	The internal voltage of the power supply module is low. The voltage low condition indicates that either the supply itself is defective or an AC power failure has occurred into the power supply module.
CsEvFormat/Event000d011c	**CsPCause/Prob000d011c**
{d "%w- %d %m-, %Y - %T"} Environment Temperature Normal condition for module in slot {I 1} reported by {m} ({t}). (event [{e}])	A chassis or cooling system problem at this device's location has been corrected.
CsEvFormat/Event000d011d	**CsPCause/Prob000d011d**
{d "%w- %d %m-, %Y - %T"} Environment Voltage Normal condition has been detected by power supply in slot {I 1} of {m} ({t}). (event [{e}])	The problem with the power supply module or AC power feed has been corrected and the unit is now functioning normally.
CsEvFormat/Event000d011e	**CsPCause/Prob000d011e**
{d "%w- %d %m-, %Y - %T"} A fan in the system's chassis has failed or is operating at an abnormal RPM rate, has been detected by {m} ({t}). (event [{e}])	Either one or more fans in the fan tray assembly have failed, or the fan tray has been removed. The situation is not critical, but temperature warm and temperature hot traps may follow. If the temperature traps have appeared in the alarm log, the failure should be addressed before overheating damages the device.
CsEvFormat/Event000d011f	**CsPCause/Prob000d011f**
{d "%w- %d %m-, %Y - %T"} A fan in the system's chassis has resumed normal operation, has been detected by {m} ({t}). (event [{e}])	The problem previously detected with the fan assembly has been corrected and the unit is now functioning normally.

Table 4-**1.**   **Device Events and Alarms**

CsEvFormat/Event000d0121	**CsPCause/Prob000d0121**
{d "%w- %d %m-, %Y - %T"} Broadcast threshold exceeded {I 1} total packets in {I 3} seconds on the module in slot {I 5} of {m} ({t}). (event [{e}])	MODULE BROADCAST THRESHOLD EXCEEDED This trap will be generated when the broadcast (packets per time interval) has been exceeded for the given module.
CsEvFormat/Event000d0122	**CsPCause/Prob000d0122**
{d "%w- %d %m-, %Y - %T"} Broadcast threshold exceeded {I 1} total packets in {I 3} seconds on port {I 7} on the module in slot {I 5} of {m} ({t}). (event [{e}])	PORT BROADCAST THRESHOLD EXCEEDED This trap will be generated when the broadcast (packets per time interval) has been exceeded for the given port.
CsEvFormat/Event000d0125	**CsPCause/Prob000d0125**
{d "%w- %d %m-, %Y - %T"} System Voltage Low condition has been detected by {m} ({t}). (event [{e}])	The internal 5 volt line of the system is low. The voltage low condition indicates that either the power supplies are failing or there is not enough power available to the host modules. This is a serious condition and should be addressed immediately.
CsEvFormat/Event000d0126	**CsPCause/Prob000d0126**
{d "%w- %d %m-, %Y - %T"} System Voltage Normal condition has been detected by {m} ({t}). (event [{e}])	The problem with the internal 5 volt line of the system has been corrected. The system voltage condition has returned to normal.
CsEvFormat/Event000d0127	**CsPCause/Prob000d0127**
{d "%w- %d %m-, %Y - %T"} An EPIM has been removed from port {I 3} on module in slot {I 1} of {m} ({t}). (event [{e}])	An Ethernet Port Interface Module (EPIM) has been physically removed.
CsEvFormat/Event000d0128	**CsPCause/Prob000d0128**
{d "%w- %d %m-, %Y - %T"} An (EPIM) has been inserted into port {I 3} on module in slot {I 1} of {m} ({t}). (event [{e}])	An Ethernet Port Interface Module (EPIM) has been physically inserted.

Table 4-1. **Device Events and Alarms**

CsEvFormat/Event000d0129	CsPCause/Prob000d0129
{d "%w- %d %m-, %Y - %T"} Traffic threshold, {I 1} packets per {I 3} seconds, exceeded on the repeater network {I 5} of {m} ({t}). (event [{e}])	The device(s) attached to this channel may have an application level problem. The attached devices may be operating properly, but the application requires a large amount of network bandwidth. If the application requires a large amount of bandwidth, a bridge or router may be used to logically separate various network segments. This trap indicates that module or port level thresholds on this repeater channel are needed to pinpoint high bandwidth users.
CsEvFormat/Event000d0130	**CsPCause/Prob000d0130**
{d "%w- %d %m-, %Y - %T"} Error threshold exceeded. An error threshold, of {I 1}% total packets in {I 5} seconds, exceeded on repeater network {I 7} of {m} ({t}). (event [{e}])	A user defined threshold has been exceeded on this channel. This threshold could indicate that a malfunctioning device is present on this channel or that a cable fault exists. A module or port level threshold should be set to further troubleshoot to the offending node.
CsEvFormat/Event000d0131	**CsPCause/Prob000d0131**
{d "%w- %d %m-, %Y - %T"} Collision threshold exceeded. The number of collisins per total packets within the time base of {I 3} seconds has been exceeded on repeater network {I 5} of {m} ({t}). (event [{e}])	A user defined threshold has been exceeded on this channel. This threshold could indicate that a malfunctioning device is present on this channel, or that a cable fault exists. Collisions are usually caused by many nodes contending for the network. As traffic rates increase, the collision rate usually follows. Therefore, if this channel has a high bandwidth utilization, a high collision rate is not unlikely. Use module and port level thresholds to further troubleshoot to a device level.
CsEvFormat/Event000d0132	**CsPCause/Prob000d0132**
{d "%w- %d %m-, %Y - %T"} Network port security is {T LockStatus 1} on repeater network {I 3} of {m} ({t}). (event [{e}])	The network administrator has changed the status of port locking for this repeater channel. The security feature locks all ports on this repeater channel so that only a valid user already in the source address table can access the network.

Table 4-1.   **Device Events and Alarms**

CsEvFormat/Event000d0133 {d "%w- %d %m-, %Y - %T"} Broadcast threshold exceeded {I 1} total packets in {I 3} seconds on repeater network {I 5} of {m} ({t}). (event [{e}])	**CsPCause/Prob000d0133** REPEATER BROADCAST THRESHOLD EXCEEDED This trap will be generated when the broadcast (packets per time interval) has been exceeded for the repeater.
CsEvFormat/Event000d0135 {d "%w- %d %m-, %Y - %T"} Port Security Status is {T LockStatus 3} for port #{I 2 }, located in port group #{I 1} of {m} ({t}). (event [{e}])	**CsPCause/Prob000d0135** PORT SECURITY STATUS This alarm is generated when a change in the lock status for a particular port occurs.
CsEvFormat/Event000d0136 {d "%w- %d %m-, %Y - %T"} Device configuration change reported by {m} ({t}). The module in slot {I 1} has been inserted.	**CsPCause/Prob000d0136** A module has been inserted into this hub.
CsEvFormat/Event000d0137 {d "%w- %d %m-, %Y - %T"} Alternate Path Repeater Management has been enabled for {m} of type {t} Network Address Synchronized to {O 1}. - (event [{e}])	**CsPCause/Prob000d0137** Alternate Path Repeater Management functionality has been enabled for this repeater model.
CsEvFormat/Event000d0138 {d "%w- %d %m-, %Y - %T"} Alternate Path Repeater Management has been enabled for {m} of type {t} No Network Address Syncronization. - (event [{e}])	**CsPCause/Prob000d0138** Alternate Path Repeater Management functionality has been enabled for this repeater model.
CsEvFormat/Event000d0139 {d "%w- %d %m-, %Y - %T"} Alternate Path Repeater Management has been disabled for {m} of type {t} Network Address Syncronized to {O 1}. - (event [{e}])	**CsPCause/Prob000d0139** Alternate Path Repeater Management functionality has been disabled for this repeater model.
CsEvFormat/Event000d013a {d "%w- %d %m-, %Y - %T"} Alternate Path Repeater Management has been disabled for {m} of type {t} No Network Address Syncronization. - (event [{e}])	**CsPCause/Prob000d013a** Alternate Path Repeater Management functionality has been disabled for this repeater model.

Table 4-1. **Device Events and Alarms**

CsEvFormat/Event000d013b {d "%w- %d %m-, %Y - %T"} Alternate Path Repeater Management has activated for {m} of type {t} Network Address changed from {O 1} to {O 2}. - (event [{e}])	**CsPCause/Prob000d013b** Router Redundancy for the managing device model has probably activated.
CsEvFormat/Event000d1139 {d "%w- %d %m-, %Y - %T"} Port Security Status is {T SecureState 3} for port #{I 2 }, located in port group #{I 1} of {m} ({t}). (event [{e}])	**CsPCause/Prob000d1139** Secured State Change This alarm is generated when the status of the secure state changes for a specific port.
CsEvFormat/Event000d113a {d "%w- %d %m-, %Y - %T"} Network Learning Status is {T LearnState 2} for the network interface #{I 1} of {m} ({t}). (event [{e}])	**CsPCause/Prob000d113a** Network Learn State This alarm is generated when network learning is reset. When learnig is reset, all secure addresses on each port, within the network, will be deleted and ports will learn source addresses again.
CsEvFormat/Event000d113b {d "%w- %d %m-, %Y - %T"} Port Group Learning Status is {T LearnState 2} for the port group #{I 1} of {m} ({t}). (event [{e}])	**CsPCause/Prob000d113b** Port Group Learn State This alarm is generated when a port group's learning is reset. When learnig is reset, all secure addresses on each port, within a port group, will be deleted and ports will learn source addresses again.
CsEvFormat/Event000d113c {d "%w- %d %m-, %Y - %T"} Port Learning Status is {T LearnState 3} for the port #{I 2}, located in port group {I 1} of {m} ({t}). (event [{e}])	**CsPCause/Prob000d113c** Port Learn State This alarm is generated when a port's learning is reset. When learnig is reset, all secure addresses on the port will be deleted and the port will learn source addresses again.
CsEvFormat/Event000d113d {d "%w- %d %m-, %Y - %T"} Network Learning Mode is {T LearnMode 2} for the network interface #{I 1} of {m} ({t}). (event [{e}])	**CsPCause/Prob000d113d** Network Learn Mode This alarm is generated when network learning mode is changed between one-time learn mode and continuous learn mode.
CsEvFormat/Event000d113e {d "%w- %d %m-, %Y - %T"} Port Group Learning Mode is {T LearnMode 2} for the port group #{I 1} of {m} ({t}). (event [{e}])	**CsPCause/Prob000d113e** Port Group Learn Mode This alarm is generated when a port group's learning mode is changed between one-time learn mode and continuous learn mode.

Table 4-1. **Device Events and Alarms**

CsEvFormat/Event000d113f	CsPCause/Prob000d113f
{d "%w- %d %m-, %Y - %T"} Port Learning Mode is {T LearnMode 3} for the port #{I 2}, located in port group {I 1} of {m} ({t}). (event [{e}])	Port Learn Mode This alarm is generated when a port's learning mode is changed between one-time learn mode and continuous learn mode.
CsEvFormat/Event00812000 {d "%w- %d %m-, %Y - %T"} ACTIVE REDUNDANT PORT FAILED - Device {m} of Type {t} reported that the current active port on interface {I 1} has failed. - (event [{e}])	No Probable cause message.
CsEvFormat/Event00812001 {d "%w- %d %m-, %Y - %T"} ACTIVATED PORT - Device {m} of Type {t} reported that a port has been activated on redundant interface {I 1}, this does not indicate the port is usable. - (event [{e}])	No Probable cause message.
CsEvFormat/Event00812002 {d "%w- %d %m-, %Y - %T"} TESTED PORT NOT USABLE - Device {m} of Type {t} reported that a port on interface {I 1} has been tested and is not usable. - (event [{e}])	No Probable cause message.
CsEvFormat/Event00812003 {d "%w- %d %m-, %Y - %T"} PRIMARY PORT SKIPPED - Device {m} of Type {t} reported that the designated primary port on interface {I 1} is unusable because Primary Revert is set to manual. - (event [{e}])	No Probable cause message.
CsEvFormat/Event00830000	No Probable cause message.
CsEvFormat/Event00830001	No Probable cause message.
CsEvFormat/Event00830002	No Probable cause message.

Table 4-1.   **Device Events and Alarms**

CsEvFormat/Event00010810	CsPCause/Prob00010810
{d "%w- %d %m-, %Y - %T"} RMON rising threshold trap received from model {m} of type {t}. AlarmIndex {I 1}, AlarmVariable {O 2}, AlarmSampleType {I 3}, AlarmValue {I 4} and AlarmRisingThreshold {I 5}. (event [{e}])	Remote Monitor Rising Alarm Threshold Exceeded This trap will be generated when the value of the trap exceeds the rising threshold for the alarm.
CsEvFormat/Event00010811	**CsPCause/Prob00010811**
{d "%w- %d %m-, %Y - %T"} RMON falling threshold trap received from model {m} of type {t}. AlarmIndex {I 1}, AlarmVariable {O 2}, AlarmSampleType {I 3}, AlarmValue {I 4} and AlarmFallingThreshold {I 5}. (event [{e}])	Remote Monitor Falling Alarm Threshold Exceeded This trap will be generated when the value of the trap exceeds the falling threshold for the alarm.
CsEvFormat/Event00010812	**CsPCause/Prob00010812**
{d "%w- %d %m-, %Y - %T"} RMON packet match trap received from model {m} of type {t}. Channel description: {S 3}. Channel had {I 2} matches. (event [{e}])	Packet Match Trap This trap will be generated when a packet is captured by a channel that is configured for sending SNMP traps.
CsEvFormat/Event003c0002	**CsPCause/Prob003c0002**
{d "%w- %d %m-, %Y - %T"} {S 1} for {m} of ({t}).	ROUTER SERVICES RECONFIGURATION RECOMMENDED ACTIONS: 1) Refer to Event Log.

Application View

This chapter describes the Application view for the ESX devices.

What Is in This Chapter

The Application view allows you to access detailed views of network information for the applications supported by the devices.

This chapter describes the following device-specific applications for the devices:

- DownLoad Application (CtDownLoadApp)
- FDDI SMT Application (FddiSMT) described in the ***Applications View Reference***

Common Applications

This device supports the following common applications described in the ***Application View Reference***:

- Bridging (CSIBridge)
  - Ethernet SDB (CT_Bdg_Enet)
  - Spanning Tree (Ct_Stp_App)
  - Static (Static_App)
  - Transparent (CT_Tp_App)
- MIB-II (SNMP2_Agent)
  - IP (IP2_App)
  - System (System2_App)
  - ICMP (ICMP_App)
  - UDP (UDP2_App)

The Standard RMON (RMONApp) application is available if you purchase it. The application is described in its management module guide.

Application View

This view shows the common and device-specific applications supported by the devices and provides access to application-specific information.

Figure 5-1 provides an example of an Application view in the Icon mode. Figure 5-2 provides an example of an Application view in the List mode.

To change the display mode, select **View** -> **Mode** -> **List** or **Icon**.

Figure 5-1.   **Example Application View (Icon Mode)**
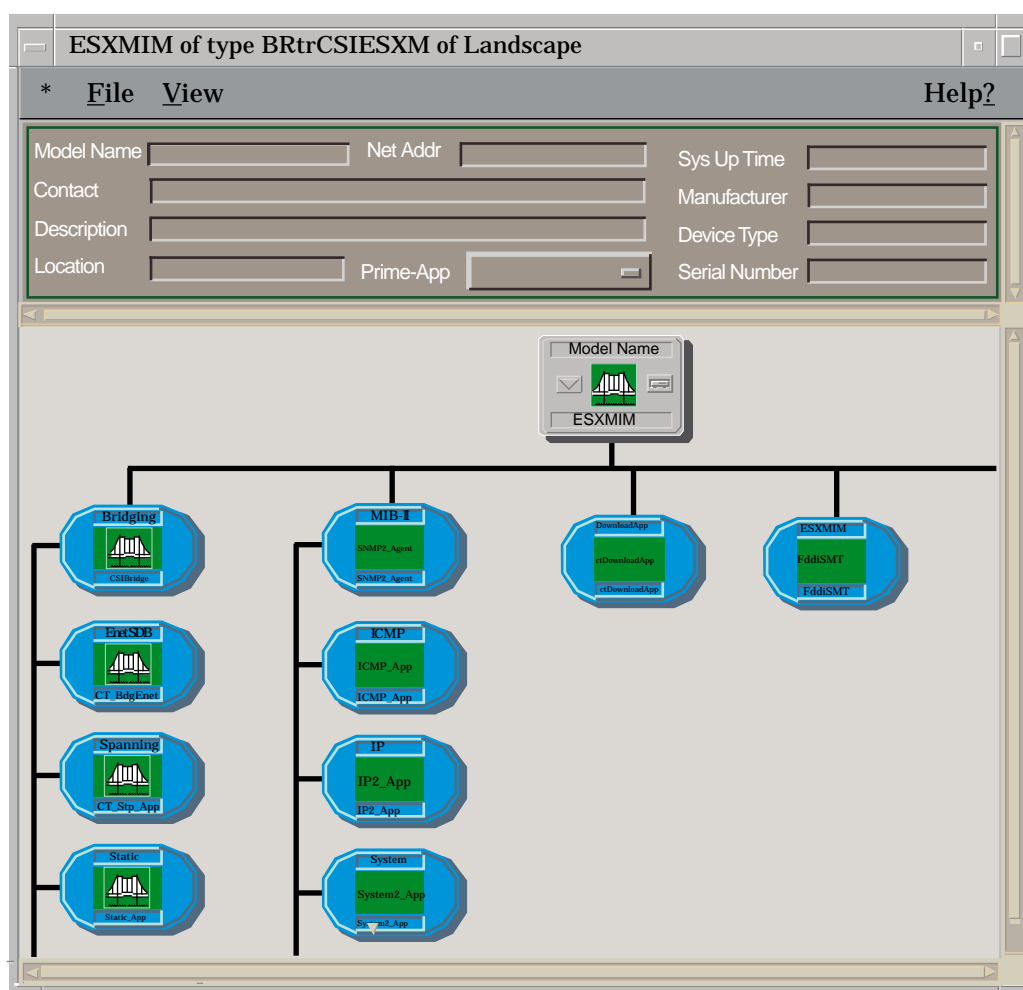
Figure 5-2.   Example Application View (List Mode)
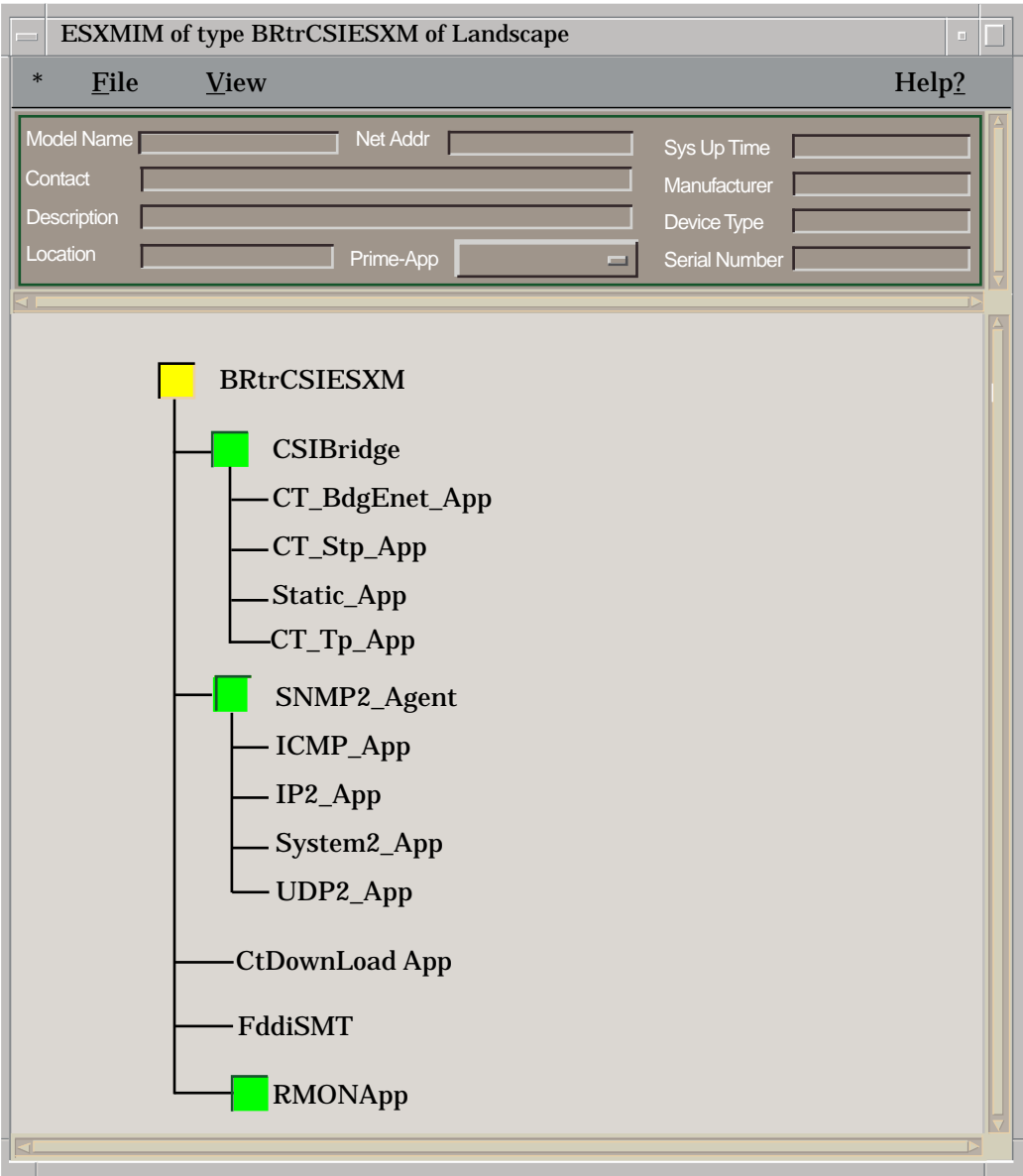
Download Application

This application provides download functionality for this device. The model type for this application is CtDownLoadApp. Access the DownLoad Application view as follows:

1. Within the Application view, highlight the CtDownLoadApp icon (Icon mode) or model type name (List mode).

2. From the Icon Subviews menu, select **Download Application**.

The Download Application view is an SPMA view and is described in the ***SPECTRUM Portable Management Application Tools Guide***.

Index